




DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	POLICY NO. 550.04	EFFECTIVE DATE 01/20/2015	PAGE 1 of 19
APPROVED BY:  Director	SUPERSEDES 500.50 01/20/2015	ORIGINAL ISSUE DATE 01/20/2015	DISTRIBUTION LEVEL(S) 1

PURPOSE

- 1.1 To ensure the confidentiality, integrity, and availability of all information entered and maintained in the Los Angeles County Department of Mental Health (LACDMH/Department) AVATAR Electronic Health Record (EHR) System.
- 1.2 To outline the acceptable use of the LACDMH AVATAR EHR System.
- 1.3 To ensure that all LACDMH workforce members are aware of their responsibilities and accountability for the protection and the confidentiality of client sensitive information viewed, maintained, and/or accessed using the LACDMH AVATAR EHR System.
- 1.4 To outline the establishment of LACDMH workforce member identities and their obligation to protect their electronic signature when signing electronic documents and forms in the AVATAR EHR System.
- 1.5 To establish a process for LACDMH workforce members to:
 - Request a new AVATAR access account;
 - Modify an existing account;
 - Deactivate an account; and/or
 - Reinstate a previously deactivated account.
- 1.6 The process described in 1.5 above is intended to maintain the confidentiality of information and the integrity of the Clinical Record as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	2 of 19

applicable federal, State, and local laws and regulations as related to confidentiality.

- 1.7 This policy applies to all software and applications comprising the LACDMH AVATAR EHR System.
- 1.8 This policy applies to all LACDMH workforce members who have or are responsible for an account in the LACDMH AVATAR EHR System.
- 1.9 This policy will be applicable to LACDMH business associates, contracted employees, consultants, volunteers, other County departments and others who have a justified business need to access the LACDMH AVATAR EHR System. Non-County employees with access to the LACDMH AVATAR EHR System who violate this policy may be subject to termination of contractual agreements, denial of access to County Information Technology (IT) resources, and other actions, including both civil and criminal penalties.

BACKGROUND

- 2.1 AVATAR is a web-based EHR management system used by LACDMH. This mission critical application contains Protected Health Information (PHI), as defined by HIPAA, and as such, strict policies regarding the account usage and monitoring of accounts must be in place to prevent unauthorized access to the system. This policy applies to all AVATAR users and outlines the processes for requesting, managing and deactivating accounts, and establishes how monitoring and tracking will take place within LACDMH (see LACDMH Policy No. 551.01, Information Access Management Policy and LACDMH Policy No. 556.01, LACDMH Acceptable Use For County Information Technology Resources Policy).

DEFINITIONS

- 3.1 **Access Control:** The act of limiting a user's access to certain data based on role or job function.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	3 of 19

- 3.2 **Account Creation:** This process of creating an account on a computer system and granting the user/authorized workforce member permission to access or use some subset of files or data. AVATAR accounts are comprised of the following components:
- 3.2.1 **User ID:** This is a unique identifier assigned to an individual's/ authorized workforce member's account. This typically contains the last name, first initial, or employee number.
 - 3.2.2 **Password:** A secret combination of characters that are either assigned to an individual/authorized workforce member or chosen by the workforce member that gives the workforce member access to the computer or network.
 - 3.2.3 **Roles:** A pre-defined set of rules that enables access to selective information in the AVATAR database based on the user's business needs.
- 3.3 **Authorized Workforce Member:** An LACDMH workforce member who has completed the official training in the use of the LACDMH Integrated Behavioral Health Information System (IBHIS); signed the County of Los Angeles Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data (see Attachment 1); signed the Confidentiality Oath (see Attachment 2); signed the LACDMH AVATAR User Security Agreement (see Attachment 3); and signed the Electronic Signature Agreement (see Attachment 4).
- 3.4 **AVATAR Super User:** LACDMH Workforce members designated at each LACDMH facility or County operated program with responsibility to disseminate and manage information and information requests relating to the AVATAR EHR System implementation.
- 3.5 **Breach:** The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the information; or where an unauthorized



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	4 of 19

person to whom such information is disclosed would not reasonably have been able to obtain such information.

3.6 **Business Associate:** An individual or entity that performs certain functions, activities, or services on behalf of LACDMH other than a member of the Department's workforce and requires the use and/or disclosure of PHI. These functions include, but are not limited to:

- Claims Processing
- Data Analysis
- IT Services
- Quality Assurance (QA)
- Billing
- Benefits Management
- Practice Management
- Legal
- Actuarial
- Document Destruction
- Claims Administration
- Accounting
- Data Aggregation
- Management Support
- Administration Support
- Accreditation
- Financial Services
- Training
- Transcription
- Consulting

3.7 **Computing Devices:** Include, but are not limited to:

3.7.1 Desktop personal computers and thin client devices.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	5 of 19

- 3.7.2 Portable computing devices, e.g., laptops, tablet computers, and mobile devices that can connect by cable, telephone wire, wireless transmission, or via any internet connection to the County's IT resources.
- 3.7.3 Portable devices, e.g., personal digital assistants (PDAs), digital cameras, smartphones, cell phones, pagers and audio/video recorders.
- 3.7.4 Portable storage media, e.g., diskettes, tapes, DVDs, CDs, USB flash drives, memory cards, and external hard drives.
- 3.7.5 Printing and scanning devices, e.g., printers, copiers, scanners, and fax machines.
- 3.7.6 Network devices, e.g., firewalls, routers, and switches.
- 3.7.7 Multiple user and application computers, e.g., servers.
- 3.8 **Confidential Data/Confidentiality:** Includes, but is not limited to, PHI and is information that is sensitive, proprietary, or personal to which access must be restricted and whose unauthorized disclosure, theft or improper use could be harmful to a person, process, or the organization. Data or information that is regarded as sensitive must be disseminated only to individuals or organizations authorized to access it.
- 3.9 **Contract:** A written agreement between the County of Los Angeles and another party (contractor and/or vendor) to provide goods or services to LACDMH under terms specified in a contract or within a verbal agreement.
- 3.10 **Data "Browsing":** The act of intentional viewing of data or records not directly within the scope of one's job functions at the time; for example, a health care provider viewing records of patients not under his or her care.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	6 of 19

- 3.11 **Electronic Signature:** For purposes of this policy, the authorized LACDMH workforce member's electronic signature will be the LACDMH user's AVATAR EHR System's identification and password.
- 3.12 **Health Insurance Portability and Accountability Act (HIPAA):** A set of standards for the privacy and security of PHI required of health plans, health care clearinghouses, and certain health care providers.
- 3.13 **Integrity:** As related to data, the quality of being complete, unimpaired, sound, and in perfect condition.
- 3.14 **Remote Access:** The ability to gain access to the LACDMH network from outside the network perimeter. Remote Access to the LACDMH AVATAR EHR System is a privilege granted through the user provisioning process to authorized workforce members as approved by LACDMH Management. Remote Access privileges granted to LACDMH Authorized Workforce Members will be restricted to the minimum necessary information required to carry out job responsibilities, terms of contracts, agreements, or as further defined by LACDMH Management. Users of Remote Access must have a Remote Access Request form on file with LACDMH Chief Information Office Bureau (CIOB).
- 3.15 **Protected Health Information (PHI):** individually identifiable information relating to the past, present, or future physical or mental health, or condition, of an individual; provision of health care to an individual; or the past, present, or future payment for health care provided to an individual.
- 3.16 **Thin Client Device:** is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional workstation, which is computer designed to take on these roles by itself. Thin Clients occur as components of a broader computer infrastructure, where many clients share their computations with the same server.
- 3.17 **Unauthorized Access, Use, or Disclosure:** For purposes of this policy, the intentional or unintentional viewing or release of sensitive information to others in



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	7 of 19

the absence of a legally permissible business need or the absence of a “need to know” by a workforce member.

- 3.18 **Workforce Member:** Employee, Business Associate, Contracted Employee, Consultant, Volunteer, other County departments and/or individual whose conduct in the performance of work for LACDMH, its offices, programs, or facilities is under the direct control of the Department, office, program, or facility regardless of whether the person is paid or unpaid.
- 3.19 For a more complete discussion of terms used in this policy, see LACDMH Policy No. 555.02, Information and Technology Security Policy, the Information Security Glossary.

POLICY

- 4.1 It is the policy of LACDMH to create, activate, manage, and monitor the usage of unique individual named user accounts and inactivate accounts when access is no longer required. This document describes the criteria and processes for account creation, account monitoring procedures, and the procedures for deactivation and reinstatement of user accounts.
- 4.2 As the AVATAR EHR System is a web-based application containing PHI, user accounts must be closely monitored and maintained to prevent unauthorized access. AVATAR user reports will be utilized to monitor appropriate access and use of this web-based system.
- 4.3 Only authorized workforce members who have completed the official training in the use of the LACDMH IBHIS and signed the following forms/documents may access PHI or Confidential Data via the LACDMH AVATAR EHR System:
- The County of Los Angeles Agreement for Acceptable Use and Confidentiality of County’s Information Technology Assets, Computers, Networks, Systems and Data;
 - The Confidentiality Oath;



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	8 of 19

- The LACDMH AVATAR User Security Agreement; and
- The Electronic Signature Agreement.

- 4.4 The Program Manager or designee will determine the level of access (Role) for each workforce member.
- 4.5 Levels of access for any individual authorized to use the LACDMH AVATAR EHR System shall be limited to the data necessary to carry out his/her specific assigned duties and responsibilities.
- 4.6 All LACDMH workforce members, whether permanent, temporary, or part-time, shall be held personally accountable for their actions or negligence in ensuring the confidentiality, integrity, and availability of LACDMH AVATAR EHR System.
- 4.6.1 LACDMH workforce members who violate this policy may be subject to appropriate disciplinary action up to and including discharge.
- 4.6.1.1 **Note:** Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5).
- 4.7 All LACDMH policies and legal requirements pertinent to confidentiality shall be maintained and observed.
- 4.8 Inquiry and/or release of client information must be in compliance with all relevant LACDMH policies (see LACDMH Policy No. 500.01, Use and Disclosure of Protected Health Information (PHI) Requiring Authorization; LACDMH Policy No. 500.02; Use and Disclosure of Protected Health Information (PHI) Without Authorization; and LACDMH Policy No. 500.03, Minimum Necessary Requirements for Using and Disclosing Protected Health Information. This is not necessarily a complete list of applicable policies, the authorized workforce members should review LACDMH policies to ensure compliance with all policies related to inquiries and release of PHI and Confidential data and information).



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	9 of 19

- 4.9 Distribution and use of reports containing PHI shall follow pertinent LACDMH privacy policies and procedures, to include clear labeling of each page as "Confidential Information."
- 4.10 No individual is permitted to copy, export, download, store, save, print screen, photograph, or video-graph displayed information from the AVATAR System without prior written authorization from LACDMH Departmental Privacy and Security Officers unless the action listed above is an approved part of conducting business as defined by the user's role. All captured information containing PHI, in paper or electronic format, must be stored or transported by departmental approved methods in accordance with LACDMH Policy No. 508.01, Safeguards for Protected Health Information and HIPAA Security/Privacy rules.
- 4.11 No workforce member shall allow any other individual to use his/her logon ID and password to access the LACDMH AVATAR EHR System.
- 4.12 Knowledge of a security violation must be reported immediately to the workforce member's supervisor.
- 4.12.1 All reports of suspected Violations of LACDMH Privacy-Related policies or of the HIPAA Privacy Standards by a workforce member shall be forwarded immediately to the designated Privacy Officer.
- 4.12.2 The Privacy Officer, or his/her designee, shall promptly conduct an investigation of the alleged violation and, as part of that investigation, shall document any known violation(s). (See LACDMH Policy No. 506.03, Responding to Breach of Protected Health Information and LACDMH Policy No. 106.13, Reporting Possible Criminal Activity)
- 4.13 Facility/Program Directors shall be responsible for taking appropriate action for any security violation with regards to PHI in the LACDMH AVATAR EHR System in their facility (see LACDMH Policy No. 506.02, Privacy Sanctions). Such action



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	10 of 19

includes notification to the LACDMH Departmental Information Security Officer or LACDMH Help Desk.

- 4.14 LACDMH shall ensure the systems and operating procedures developed and operated by and for LACDMH contain internal and external controls to ensure there is no concentration of authority sufficient for one individual to commit undetected malicious or fraudulent acts.
- 4.15 LACDMH management shall cultivate and maintain a high level of employee awareness of the importance of data security. Employee awareness shall consist of a signed acknowledgement of responsibility under this policy and other such security policies and procedures that LACDMH has implemented.

PROCEDURE

5.1 New Account Creation:

5.1.1 LACDMH workforce members, business associates, contracted employees, consultants, volunteers, other County departments requesting an AVATAR account must:

5.1.1.1 Acknowledge that they have read and understand this policy and procedure (LACDMH Policy No. 550.04, Access to Integrated Behavioral Health Information System Using AVATAR Electronic Health Record System); and

5.1.1.2 Complete official training in the use of the IBHIS; and

5.1.1.3 Sign:

- The County of Los Angeles Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data;
- The Confidentiality Oath;



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	11 of 19

- The LACDMH AVATAR User Security Agreement; and
- The Electronic Signature Agreement.

5.1.1.4 These requirements may be met as part of hiring orientation or upon the implementation of the AVATAR EHR system. All required documentation will be available for review and audit, for compliance investigations, and for routine reviews by the Departmental Security Officer, Compliance, Privacy, and Audit Services Bureau (CPAS), QA, or auditors.

5.1.2 To ensure uninterrupted access to the LACDMH AVATAR EHR System, all users must renew their admittance annually by:

5.1.2.1 Acknowledging that they have read and understood the LACDMH Policy 550.04, Access to Integrated Behavioral Health Information System (IBHIS) Using AVATAR Electronic Health Record System; and

5.1.2.2 Re-signing:

- The County of Los Angeles Agreement for Acceptable Use and Confidentiality of County's Information Technology Assets, Computers, Networks, Systems and Data;
- The Confidentiality Oath;
- LACDMH AVATAR User Security Agreement; and
- The Electronic Signature Agreement.

5.1.2.3 The renewal process will be through the LACDMH workforce member's Annual Report of Performance Evaluation packet.

5.1.3 Any requests for exceptions due to unique user or program responsibilities must be reviewed and approved by the Departmental Information Security Officer. Record of decision and type of access will be maintained in the AVATAR account management folder.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	12 of 19

- 5.1.4 Account management policies apply to all AVATAR users, regardless of type of funding or contract.
- 5.1.5 Uniquely named accounts are created upon the completion of the account request procedure outlined below. AVATAR user accounts are made of three components:
- User ID;
 - Password; and
 - User Role.
- 5.1.6 An individual is eligible for an AVATAR user account if all of the following conditions are met:
- 5.1.6.1 The individual is a current LACDMH workforce member, business associate, contracted employee, consultant, volunteer, or in another County department;
- 5.1.6.2 Access to AVATAR is required in order to complete necessary job functions;
- 5.1.6.3 Has completed a request or change authorization for an AVATAR account approved by his/her supervisor; and
- 5.1.6.4 Has completed the requirements in 5.1 above.
- 5.1.7 After the creation and use of an AVATAR account, if any of the conditions in 5.1.6 change, the individual is no longer eligible for an AVATAR user account. Examples include separation from employment and/or a change in job function that no longer requires access to the AVATAR Electronic Health Record System. Accordingly, the account inactivation process (see 5.2 below) outlined in this policy must be immediately followed.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	13 of 19

5.1.8 A workforce member's access may be limited or denied based on monitoring, investigation, follow-up, and action.

5.2 Account Deactivation:

5.2.1 If any of the following conditions are met, an AVATAR account must be deactivated:

5.2.1.1 Separation of a workforce member from LACDMH;

5.2.1.2 Interdepartmental transfer or relocation of workforce member from one program / unit / division / bureau to another;

5.2.1.3 Extended Leave of Absence ninety (90) days or longer;

5.2.1.4 Access is no longer required to complete job functions; and/or

5.2.1.5 Due to an audit, monitoring, compliance, investigation, and/or breaches.

5.2.2 In order to deactivate an AVATAR account, a completed service catalog request or change authorization must be submitted by the workforce member's supervisor. This request must indicate the last date that the AVATAR EHR System is required. Access will be terminated effective this date.

5.3 Account Reinstatement:

5.3.1 In the event a deactivated AVATAR account needs to be reinstated:

5.3.1.1 and it is less than ninety (90) days since the deactivation date, a service catalog request or change authorization for an AVATAR account approved by the workforce member's supervisor must be submitted.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	14 of 19

5.3.1.2 and it is greater than ninety (90) days since the deactivation date, the workforce member will be required to complete training before reinstatement of the account.

5.4 Access Control and Audit:

5.4.1 Access to data contained within the AVATAR EHR System is controlled by the creation and maintenance of Roles within the AVATAR EHR System. There is a minimum of one role per workforce member.

5.4.2 LACDMH periodically audits access to data within the AVATAR EHR System. All access must be on a “need to know basis” in accordance with HIPAA Privacy/Security rules. Data browsing is strictly prohibited.

5.4.3 Audit logs will be maintained for a minimum of one year and available for routine and special audits or investigations as required or determined by the Administration Deputy, the Departmental Compliance Officer, or designee. AVATAR reports may also be utilized as needed to validate appropriate use of the system.

5.4.3.1 When responding to a request for release of information related to a particular clinical record, the audit log associated with that record and/or the identification of staff who have accessed this record will only be released when the Department is legally required to provide the audit log associated with that record and/or to identify staff who accessed that clinical record (e.g., when the request explicitly asks for the audit log and/or for LACDMH to identify all staff who accessed the record). If the Department is required to release the audit log and/or identify staff who have accessed a specific medical record, the Department will restrict its response to that which is legally required to comply with the parameters of the request (e.g., treating staff only).



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	15 of 19

- 5.4.4 LACDMH requires periodic verification of current accounts from AVATAR Super Users. This requires an explicit acknowledgement that the account's role is accurately assigned and is appropriately utilized.
- 5.4.5 LACDMH Information Security will provide cyclical reports identifying accounts that have not been used within the preceding ninety (90) days.
- 5.4.6 AVATAR accounts will be inactivated after ninety (90) days of inactivity.
- 5.4.7 AVATAR Super Users will be responsible for providing confirmation of account users based on these reports within **five (5) business days** of receiving the reports.
- 5.4.8 AVATAR reports will be utilized to audit user activity.

5.5 Password Protection:

- 5.5.1 LACDMH abides by the following standards with regard to password protection:
 - 5.5.1.1 Passwords must have a minimum length of eight (8) characters; and
 - 5.5.1.2 Must meet at least three (3) out of the four (4) following requirements:
 - Contain at least one (1) lower case letter (a through z);
 - Contain at least one (1) upper case letter (A through Z);
 - Contain at least one (1) base ten (10) digit (0 through 9); and
 - Contain at least one (1) special character such as % or *.
- 5.5.2 Passwords may not contain the user's first or last name.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	16 of 19

- 5.5.3 Minimum password age is set to two (2) days.
- 5.5.4 Maximum password age is set to ninety (90) days. Passwords on all LACDMH systems must be changed, at a minimum, every ninety (90) days.
- 5.5.5 Password expiration reminders are set to be sent fourteen (14) days prior to expiration date and every time the user initiates a logon.
- 5.5.6 The reuse of the last six (6) passwords is prevented. Accordingly, a history of previously used passwords is maintained.
- 5.5.7 Unique initial passwords must be provided through a secure and confidential manner, and initial passwords must be changed upon first logon.
- 5.5.8 After five (5) unsuccessful consecutive logon attempts (e.g., incorrect passwords), the user's account will become automatically locked, and the user must contact the Help Desk for account unlocking.
- 5.5.9 Passwords should never be written down and left in plain sight or stored in plain text online. If a password must be written down, it should be stored in a secure location.
- 5.5.10 Users must prevent passwords from being known or used by others.
- 5.5.11 Users must log off from applications when done using them.
- 5.5.12 Users must secure workstations when they are away from them. Devices will automatically lock for inactivity after twenty (20) minutes.
- 5.5.13 Users must never use the "Remember Password" feature for any application.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	17 of 19

5.5.14 Users must report suspected password compromises.

5.5.15 Users must contact the Help Desk if they believe someone has obtained their password.

5.5.16 Users must change their password if they suspect it has been compromised.

5.6 Remote Access:

5.6.1 LACDMH workforce members authorized for connecting remotely to LACDMH AVATAR EHR System must ensure the following controls are implemented:

5.6.1.1 The remote computing device being used must be protected with a password;

5.6.1.2 A firewall must be activated and configured on the remote computing device;

5.6.1.3 The remote computing device being used must be running the vendor-supported operating system that is automatically updated and has up-to-date security patches installed;

5.6.1.4 Vendor-supported anti-virus, anti-spyware must be installed to perform continuous and/or scheduled scanning to detect malware or malicious activities. The virus definition list must be updated at least once daily;

5.6.1.5 The remote computing device must be configured to lock after twenty (20) minutes of inactivity;

5.6.1.6 The remote computing device must be physically protected and not shared with unauthorized persons;



**LAC
DMH**
LOS ANGELES COUNTY
DEPARTMENT OF
MENTAL HEALTH

DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	18 of 19

- 5.6.1.7 The displayed information cannot be visible to any unauthorized person;
- 5.6.1.8 The remote computing device must be locked or logged off while unattended;
- 5.6.1.9 Access to PHI over a wireless connection is prohibited unless via a secure and encrypted connection;
- 5.6.1.10 When emailing confidential information from a remote computing device, LACDMH workforce members must use the LACDMH secure messaging system in accordance with LACDMH Policy 557.02, Appropriate Use of Email for Transmitting PHI and Confidential Data; and
- 5.6.1.11 Remote LACDMH workforce members are prohibited from using or printing paper documents that contain PHI unless this action is an approved part of conducting business as defined by the user's role. Paper documents containing PHI must be appropriately stored or transported in accordance with LACDMH Policy 508.01, Safeguards for Protected Health Information (PHI). Electronic documents containing PHI must be encrypted prior to storage or transportation.

AUTHORITY

1. HIPAA Security Rule – 45 Code of Federal Regulations (CFR) Parts 160 and 164.
2. Board of Supervisors Policies: 6.101 - Use of County Information Technology Resources



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT	POLICY NO.	EFFECTIVE DATE	PAGE
ACCESS TO INTEGRATED BEHAVIORAL HEALTH INFORMATION SYSTEM USING AVATAR ELECTRONIC HEALTH RECORD SYSTEM	550.04	01/20/2015	19 of 19

ATTACHMENTS (HYPERLINKED)

1. [County of Los Angeles Agreement for Acceptable Use and Confidentiality of County Information Technology Resources](#)
2. [Confidentiality Oath - LACDMH Workforce Members](#)
3. [LACDMH AVATAR User Security Agreement](#)
4. [Electronic Signature Agreement](#)

REFERENCES

1. LACDMH Policy No. 106.13, Reporting Possible Criminal Activity
2. LACDMH Policy No. 500.01, Use and Disclosure of Protected Health Information (PHI) Requiring Authorization
3. LACDMH Policy No. 500.02, Minimum Necessary Requirements for Using and Disclosing Protected Health Information (PHI) Without Authorization.
4. LACDMH Policy No. 500.03, Minimum Necessary Requirements for Using and Disclosing Protected Health Information
5. LACDMH Policy No. 506.02, Privacy Sanctions
6. LACDMH Policy No. 508.01, Safeguards for Protected Health Information (PHI)
7. LACDMH Policy No. 506.03, Responding to Breach of Protected Health Information
8. LACDMH Policy No. 551.01, Information Access Management Policy
9. LACDMH Policy No. 556.01, LACDMH Acceptable Use for County Information Technology Resources Policy
10. LACDMH Policy No. 555.02, Information and Technology Security Policy
11. LACDMH Policy No. 557.02, Appropriate Use of Email for Transmitting PHI and/or Confidential Data

RESPONSIBLE PARTY

Los Angeles County Department of Mental Health - Chief Information Office Bureau